

# <sup>1</sup>Lion's Roar in SEA: Singaporean Way in Increasing the Awareness of Cybersecurity<sup>2</sup>

Aufar M. Rizki

Undergraduate Student of International Relations Department at Universitas Katolik Parahyangan  
aufar11rizki@gmail.com

## Abstrak

Nowadays, where almost all aspect are digitilized have caused a massive increase of cyber threats which is a tangible threats for human beings. However, cybersecurity still has a second priority to accomplish for mostly countries, just few country who put big concern to this issue. As the Chair of ASEAN 2018, Singapore has made a project in strengthening the collective resillience of cybersecurity. The goal of this project is to increase the awareness of ASEAN countries in tackling cyberthreats in which it endangers the cybersecurity

**Keywords:** cybersecurity<sup>3</sup>, cyberthreats<sup>4</sup>, Singapore, ASEAN.

---

## Pendahuluan

Manusia sebagai makhluk yang dianugerahi akal dan pikiran oleh Tuhan Yang Maha Esa, senantiasa bekerja dan berpikir terkait hal yang di sekitarnya. Hasil dari pemikiran dan pekerjaan manusia ini sejatinya akan menghasilkan sebuah produk yang dapat meringankan manusia lain untuk bekerja dan melakukan aktivitas lainnya. Dalam kehidupannya, manusia secara bertahap mengembangkan produk untuk memudahkan segala pekerjaan. Produk yang

---

<sup>1</sup> Tulisan ini merupakan pelengkapan dan perbaikan dari makalah yang dipresentasikan oleh penulis sebagai pemakalah pada acara Seminar Nasional Politik dan Hubungan Internasional (SENAS POLHI) 2018 yang diselenggarakan oleh Universitas Wahid Hasyim di Sampangan, Semarang, Jawa Tengah pada tanggal 30 Agustus 2018. Makalah yang penulis sertakan pada SENAS POLHI 2018 telah dipublikasikan melalui "Prosiding SENAS POLHI Volume 1. No.1 (2018) dengan nomor ISBN: 978-602-8273-63-3, serta nomor e-ISBN: 978-602-8273-64-0.

<sup>2</sup> Judul tulisan ini juga mengalami perubahan dari naskah makalah yang dipresentasikan penulis pada kegiatan SENAS POLHI 2018 sebagaimana telah penulis paparkan pada catatan kaki sebelumnya. Judul Makalah yang penulis sertakan pada SENAS POLHI 2018 adalah "Langkah Singapura dalam Meningkatkan Kesadaran Negara Anggota ASEAN untuk Meningkatkan Keamanan Siber".

<sup>3</sup> Cybersecurity kemudian dialihbahasakan menjadi "keamanan siber".

<sup>4</sup> Cyberthreats kemudian dialihbahasakan menjadi "ancaman siber".

mempermudah pekerjaan manusia itu dinamakan teknologi. Definisi ini merupakan penjelasan dasar dari mengapa manusia menciptakan teknologi. Teknologi semakin berkembang seiring perkembangan zaman. Teknologi mengalami salah satu pencapaian terbesarnya ketika James Watt mematenkan hasil penemuannya yakni mesin uap pada tahun 1775 di Inggris.<sup>5</sup> Setelah penemuan besar itu, teknologi berkembang pesat hingga akhirnya melahirkan sebuah revolusi industri, karena adanya penciptaan mesing-mesin produksi secara massal di Inggris pada saat itu.<sup>6</sup> Sejak saat itu teknologi terus mengalami perkembangan hingga saat ini di era millennial. Saat ini, acap kali kita mendengar bagaimana menghadapi perkembangan teknologi di generasi keempat atau sering disebut dengan “Teknologi 4.0”. Teknologi 4.0 ialah generasi teknologi yang keempat dimana teknologi yang digunakan sudah menggunakan internet.<sup>7</sup> Segala sesuatu telah bergantung pada internet, atau disebut dengan *Internet of Things*.<sup>8</sup> Dalam era yang disebut *Internet of Things* ini, tiap manusia satu dengan yang lainnya atau benda-benda di sekitarnya dapat terkoneksi satu sama lain dengan jaringan internet.<sup>9</sup> Saat ini sudah dapat kita rasakan bagaimana antara manusia satu dengan yang lainnya sudah dapat terkoneksi dengan jaringan internet. Koneksi internet ini dibangun oleh benda-benda yang ada disekitar manusia seperti gawai, tablet hingga *laptop*. Dengan perkembangan zaman seperti ini, hampir seluruh aspek dalam kehidupan kita telah dapat terkoneksi dengan jaringan internet. Dengan kata lain, internet merupakan teknologi mutakhir yang diciptakan manusia untuk memudahkan pekerjaan manusia. Internet berperan sebagai media dalam setiap sektor kehidupan masa kini. Dari sektor politik, ekonomi, perdagangan, pendidikan, hingga pertahanan semuanya telah terdigitalisasi. Tentu dengan adanya digitalisasi menghadirkan banyak keuntungan karena meningkatnya efektivitas dan efisiensi dalam setiap sektor. Digitalisasi ini tentunya relevan dengan perkembangan zaman saat ini. Karena disamping penggunaan internet yang semakin massal dalam sektor formal, masyarakat luas pun telah terbiasa dengan penggunaan internet dalam kehidupan sehari-hari. Dalam lingkup Asia Tenggara, angka penggunaan internet sudah terbilang tinggi. Tercatat

---

<sup>5</sup> Christopher McFadden. Interesting Engineering “James Watt, Father of The Modern Steam Engine”. Culture/Biography. 30 Desember 2017. Diakses pada 18 Juli 2018. <https://interestingengineering.com/james-watt-father-of-the-modern-steam-engine>

<sup>6</sup> Ibid.

<sup>7</sup> Fadly Fauzi Rachman. DetikFinance. “Apa itu Teknologi 4.0?”. 4 April 2018. Diakses pada 18 Juli 2018. <https://finance.detik.com/industri/d-3952668/apa-itu-revolusi-industri-40>

<sup>8</sup> Ibid.

<sup>9</sup> Jacob Morgan. Forbes. “A Simple Explanation of ‘The Internet of Things’ “. 13 Mei 2014. Diakses pada 18 Juli 2018. <https://www.forbes.com/sites/jacobmorgan/2014/05/13/simple-explanation-internet-things-that-anyone-can-understand/>

saat ini pengguna internet di Asia Tenggara mencapai 330 juta jiwa.<sup>10</sup> Menurut data yang diambil dari *Worldometers*, Penduduk Asia Tenggara saat ini mencapai 656 juta jiwa.<sup>11</sup> Artinya lebih dari setengah masyarakat Asia Tenggara telah menggunakan Internet dalam kehidupan sehari-harinya. Mereka telah merasakan dampak dari dunia yang terdigitalisasi. Sebanyak 48,2% dari populasi masyarakat Asia Tenggara bermukim di wilayah urban.<sup>12</sup> Maka, masyarakat sejumlah persentase itulah yang mendapatkan jaminan terhadap akses pada koneksi jaringan internet. Penggunaan internet secara massal memang tidak terbantahkan lagi. Fenomena ini tentunya memberikan keuntungan yang sangat besar, salah satunya yang paling berdampak ialah pada sektor ekonomi dan perdagangan. Saat ini, Asia Tenggara tercatat sebagai pasar ketujuh terbesar di dunia dengan *Gross Domestic Product* (GDP) \$2,7 Milyar dengan pertumbuhan mencapai 5,2%.<sup>13</sup> Ini membuktikan bahwa kawasan Asia Tenggara merupakan kawasan yang strategis dalam hal perdagangan, terlebih setelah adanya digitalisasi ekonomi yang semakin mempermudah adanya transaksi lintas batas negara. Penggunaan internet yang semakin massal, seperti yang telah dipaparkan sebelumnya, juga membantu digitalisasi ekonomi saat ini. Berdasarkan laporan dari *Google* dan *Temasek*, regional Asia Tenggara siap memimpin dalam hal penggunaan internet tertinggi di dunia.<sup>14</sup> Asia Tenggara memiliki 641 juta konsumen pada tahun 2017 lalu, dan 51% diantaranya merupakan pengguna internet aktif.<sup>15</sup> Ini menandakan bahwa penggunaan internet yang luas juga dimanfaatkan untuk melakukan transaksi perdagangan, sebagaimana kemudahan yang saat ini didapatkan. Kemudahan ini didapatkan ketika segalanya dapat dioperasikan melalui ponsel pintar. Masih dari sumber yang sama, dikatakan bahwa 90% dari pengguna internet di kawasan Asia Tenggara mengakses internet melalui ponsel mereka.<sup>16</sup> Maka Asia Tenggara merupakan pasar ketiga terbesar di dunia dalam aspek ekonomi digital.<sup>17</sup>

---

<sup>10</sup> Daniel. PPC Land. "Southeast Asia Internet Users are Booming". 4 Mei 2018. Diakses pada 20 Juli 2018. <https://ppc.land/southeast-asia-internet-users-are-booming/>

<sup>11</sup> Worldometers. "South Eastern Asia Population". 20 Juli 2018. Diakses pada 20 Juli 2018. <http://www.worldometers.info/world-population/south-eastern-asia-population/>

<sup>12</sup> Ibid.

<sup>13</sup> Justina Lee. Business Trend, Nikkei, Asian Review. "ASEAN Remains "Prime Target" for Cyberattacks". 8 Februari 2018. Diakses pada 20 Juli 2018. <https://asia.nikkei.com/Business/Business-Trends/ASEAN-remains-prime-target-for-cyberattacks>

<sup>14</sup> Rayna Hollander. Business Insider. "Southeast Asia Could be a Leader in Mobile Internet User Next Year". 13 Desember 2017. Diakses pada 20 Juli 2018. <http://www.businessinsider.com/southeast-asia-could-be-a-leader-in-mobile-internet-usage-next-year-2017-12/?IR=T>

<sup>15</sup> Ibid.

<sup>16</sup> Ibid.

<sup>17</sup> Ibid.

Dengan fakta yang telah dipaparkan sebelumnya, bahwa penggunaan internet yang sangat masif, serta keterlibatan sektor lain salah satunya ekonomi terhadap dunia digital, menghadirkan suatu permasalahan baru yakni keamanan terkait dunia digital itu sendiri. ASEAN pada tahun ini telah menekankan pada pembangunan ekonomi digital sebagai salah satu prioritas pembangunan regional.<sup>18</sup> Dengan rencana pengembangan pada bidang ekonomi digital, maka negara-negara ASEAN juga harus membuat kebijakan khusus terkait keamanan digital termasuk pada sektor pemerintahan.<sup>19</sup> Keamanan di dunia digital ini lebih sering disebut dengan *Cybersecurity* atau keamanan siber. Dewasa ini keamanan siber merupakan sektor baru di bidang pertahanan yang mulai mendapatkan perhatian khusus. Keamanan siber tergolong ke dalam keamanan negara non tradisional. Sebab ancaman yang dihadapi dari ancaman siber ini bukan lagi ancaman konvensional yang mengancam keadulatan atau wilayah teritori negara, melainkan ancaman yang mengancam ketahanan siber suatu negara. Jika siber suatu negara mengalami masalah atau penyerangan dari pihak lain, maka ini akan menyebabkan permasalahan sistem jaringan dan koneksi antar *devices* dari satu komputer ke komputer lainnya. Jika hal ini terganggu, maka seluruh aktifitas yang terdigitalisasi akan mengalami hambatan, tidak dapat serta merta diperbaiki dalam waktu yang singkat. Maka dari itu banyak negara sudah melihat itu sebagai ancaman nyata dan berusaha untuk meningkatkan keamanan siber. Bagi kawasan Asia Tenggara, negara – negara anggota ASEAN telah menganggap serius permasalahan ini. Sebagian telah berkomitmen tinggi untuk menginvestasikan anggaran negaranya untuk pengamanan dibidang siber tersebut. Dalam sektor keamanan siber ini, sebenarnya aktor negara bukanlah pihak yang paling kuat dalam menghadapi ancaman siber, karena aktor *non-state* sebenarnya lebih memiliki andil besar dalam kontribusinya baik sebagai tokoh dibalik penyerangan siber maupun aktor yang dapat memberantas serangan siber.<sup>20</sup> Maka, seyogianya negara harus melakukan kerjasama juga dengan pihak swasta yang bergerak di bidang keamanan siber. Di tahun 2018 ini, dengan Singapura sebagai *Chairmanship* ASEAN, telah menegaskan akan membangun kawasan yang berkomitmen akan keamanan siber. ASEAN di bawah Singapura berkomitmen untuk membangun kawasan yang fleksibel dan inovatif terhadap perubahan situasi global yang

---

<sup>18</sup> Oleg Abdurashitov. KasperskyLab. “ASEAN Cyber Diplomacy: Overcoming Differences”. 30 Oktober 2018. Diakses pada 7 Desember 2018. <https://www.kaspersky.com/about/policy-blog/general-cybersecurity/asean-cyber-diplomacy-overcoming-differences>

<sup>19</sup> Ibid.

<sup>20</sup> Anastasiya Kazakova. KasperskyLab. “What’s To Be Done About The Militarization of Cyberspace? More Cooperation With Each Other”. 30 Oktober 2018. Diakses pada 6 Desember 2018. <https://www.kaspersky.com/about/policy-blog/general-cybersecurity/how-to-deal-with-militarizing-cyberspace>

cepat berdasarkan *ASEAN Leaders' Vision for a Resilient and Innovative ASEAN*.<sup>21</sup> Lebih Spesifik lagi, ASEAN mengadopsi *ASEAN Leaders' Statement on Cybersecurity Cooperation*, dengan kesadaran akan pentingnya meningkatkan keamanan dalam sektor dunia maya dalam menghadapi urgensi ancaman siber.<sup>22</sup> ASEAN telah mengangkat aspek *cybersecurity* menjadi sebuah agenda kebijakan regional tahun ini, dengan berusaha melakukan investasi dalam bidang teknologi yang tepat serta membangun kemitraan dengan lembaga ahli terkait.<sup>23</sup>

### Rumusan Masalah

Dengan perkembangan teknologi yang semakin mutakhir, munculnya dunia digital membawa perubahan, yakni adanya digitalisasi di hampir seluruh aspek kehidupan manusia. Mulai dari kehidupan sosial, kesehatan, hingga penanaman identitas manusia menjadi wilayah dari dunia digital.<sup>24</sup> Digitalisasi juga berlaku pada sektor kenegaraan seperti bidang pemerintahan dan pertahanan. Dengan munculnya fenomena ini maka lahir suatu permasalahan baru yang harus dihadapi setiap negara, yaitu masalah terkait keamanan akses dari sistem digital tersebut. Keamanan Siber memang merupakan aspek baru dalam lingkup pertahanan, namun tidak sedikit negara maupun aktor internasional lain yang menganggap permasalahan ini memiliki urgensi yang tinggi. ASEAN sebagai organisasi regional di Asia Tenggara termasuk salah satunya yang berkomitmen tinggi dalam menangkal ancaman keamanan siber. Maka melalui tulisan ini penulis hendak membahas “bagaimana langkah Singapura dalam meningkatkan kesadaran negara negara ASEAN terhadap ancaman siber?”, terkait dengan Singapura sebagai *Chair ASEAN* di tahun 2018 ini.

---

<sup>21</sup> “32nd ASEAN Summit – Chairman Statement”. ASEAN Singapore 2018. Resilient and Innovative, Press Release. 28 April 2018. Diakses pada 20 Juli 2018. [https://www.asean2018.sg/Newsroom/Press-Releases/Press-Release-Details/20180428\\_Chairmans\\_Statement](https://www.asean2018.sg/Newsroom/Press-Releases/Press-Release-Details/20180428_Chairmans_Statement)

<sup>22</sup> Ibid.

<sup>23</sup> John Brandon. The Asia Foundation. “Why ASEAN Needs to Invest More In Cybersecurity”. 9 Mei 2018. Diakses pada 8 Desember 2018. <https://asiafoundation.org/2018/05/09/why-asean-needs-to-invest-more-in-cybersecurity/>

<sup>24</sup> Barbara Morsello. European Association for The Study of Science and Technology. “Digitalization of Life – How Technology Redefine The Self in The Global Context”. *EASST Review*. Volume 35(4). Desember 2016. Diakses pada 5 November 2018. <https://easst.net/article/digitalization-of-life-how-technology-redefine-the-self-in-the-global-context/>

## Landasan Teori

ASEAN merupakan organisasi regional yang berada di Asia Tenggara. ASEAN Setiap tahunnya memiliki pemimpin atau disebut *Chair*. *Chair* ASEAN ini akan berganti pada setiap tahunnya. Pada tahun 2018 ini Singapura berkesempatan menjadi *Chair* ASEAN. Sebagaimana ASEAN adalah organisasi yang mewadahi negara – negara, aka pemimpin dari ASEAN ialah seorang kepala negara dari negara yang menjadi *Chair* di tahun tersebut. Maka, pada tahun ini, Lee Hsien Loong merupakan pemimpin ASEAN, sebab beliau adalah Perdana Menteri Singapura saat ini. Lee memiliki beberapa terobosan demi mewujudkan ASEAN yang lebih baik. Jargon yang dibawa oleh Singapura ialah “Resilient and Innovative”.<sup>25</sup> Tujuan yang ingin dibawa oleh Singapura ialah membangun keamanan kolektif antara negara – negara ASEAN di bidang terorisme, ancaman siber dan pemanasan global.<sup>26</sup> Ketiga bidang ini memang diprogramkan oleh Singapura untuk ASEAN di tahun ini, dengan tujuan untuk mencapai ASEAN yang inovatif, termasuk dengan penggunaan ekonomi digital.<sup>27</sup>

Ekonomi digital memang merupakan urgensi yang sedang dibangun oleh masyarakat ASEAN, karena sektor ini merupakan sektor yang sedang beranjak naik dengan angka pengguna yang tinggi. Dengan tingginya pengguna internet, semakin merambah pula penggunaan internet ini ke bidang ekonomi. Betapa tingginya penggunaan ekonomi digital, di Indonesia sendiri sebagai salah satu pengguna internet terbesar memiliki investasi asing yang tinggi di bidang ekonomi digital. Tahun lalu investasi asing di bidang ekonomi digital di Indonesia sebesar 51,75 juta dollar AS.<sup>28</sup> Selain itu, angka penggunaan internet di Asia Tenggara memang telah menunjukkan angka yang tinggi. Pada 2017, tercatat pengguna internet aktif di Asia Tenggara sejumlah 339,2 juta jiwa dari total 644,1 juta jiwa masyarakat yang tinggal di regional tersebut.<sup>29</sup> Jumlah tersebut menunjukkan pengguna internet telah mencapai 53%.<sup>30</sup> Dengan jumlah pengguna media sosial aktif ialah 305,9 juta jiwa.<sup>31</sup> Data-data tersebut menunjukkan bahwa penggunaan internet dalam berbagai bidang termasuk

---

<sup>25</sup> ASEAN Singapore 2018. Resilient and inovative. “Experience ASEAN Festival – Opening Remarks by Prime Minister Lee Hsien Loong”. 13 Januari 2018. Diakses pada 31 Juli 2018. <https://www.asean2018.sg/MFA/Newsroom/Press-Releases/Press-Release-Details/20180112>

<sup>26</sup> Ibid.

<sup>27</sup> Ibid.

<sup>28</sup> Donny Fernando. The Jakarta Post. “Indonesia Records \$4,8 Billion in Digital Economy”. 13 Januari 2018. Diakses pada 30 Juli 2018. <http://www.thejakartapost.com/news/2018/01/31/indonesia-records-4-8-billion-investment-in-digital-economy.html>

<sup>29</sup> Simon Kemp. Hootsuite. We Are Social. TechInAsia. “The Full Guide to Southeast Asia Digital Landcsape in 2017” 8 Februari 2017. Diakses pada 2 Agustus 2018. <https://www.techinasia.com/talk/full-guide-southeast-asia-digital-landscape-2017>

<sup>30</sup> Ibid.

penggunaan media sosial aktif di Asia Tenggara ini telah mencapai angka yang tinggi untuk sebuah regional yang didominasi oleh negara berkembang. Dengan fakta seperti itu, maka konsekuensi yang didapat dari penggunaan internet yang tinggi juga cukup besar. Semakin tinggi angka penggunaan internet oleh masyarakat, maka semakin tinggi juga konsekuensi akan ancaman yang didapat. Konsekuensi yang diterima dari tingginya ancaman terhadap dunia digital seperti peretasan sistem komputer, pencurian data identitas hingga ancaman pada setiap transaksi *e-commerce*.<sup>32</sup> Ancaman pada dunia siber ini jelas nyata dampaknya. Salah satu yang paling berdampak ialah ancaman pada sektor bisnis digital atau biasa disebut dengan *e-commerce*. *E-commerce* menanggung risiko yang sangat besar terhadap ancaman siber. Misalkan saja, ketika situs perdagangan mereka diretas oleh pihak lain dan tidak dapat dibuka, maka kepercayaan konsumen akan menurun secara signifikan dan mengurangi minatnya untuk berbelanja pada situs tersebut di masa yang akan datang.<sup>33</sup>

*Cybersecurity* atau keamanan siber ini memiliki definisi suatu proteksi yang berbasis koneksi internet dari serangan siber termasuk *hardware*, *software* dan data.<sup>34</sup> Permasalahan utama dari keamanan siber ini ialah kompleksitas resiko yang dimiliki terhadap serangan dari pihak luar yang mengancam keamanan data dan sistem komputer.<sup>35</sup> Namun objek yang paling mendasar dari keamanan siber ialah keamanan sumber daya yang ada pada sistem siber yaitu data, baik dari segi integritas data, ketersediaan hingga kerahasiaan data.<sup>36</sup> Bidang kajian ini lahir akibat dari meningkatnya angka serangan siber, sehingga adanya kebutuhan untuk mensekuritisasi kumpulan data serta informasi lain yang berkaitan dengan perusahaan atau negara, maka muncul lah kajian *cybersecurity* ini.<sup>37</sup> Sistem dari keamanan siber ini penting untuk diketahui banyak sektor, termasuk pada kehidupan sehari-hari. Seperti telah diuraikan pada bagian pendahuluan, bahwa keamanan siber ini memiliki andil yang besar dalam seluruh aspek kehidupan. Sektor kehidupan sehari-hari, ekonomi, keamanan *database*, hingga sektor pemerintahan menjadi aspek penelitian dalam tulisan ini.

---

<sup>31</sup> Ibid.

<sup>32</sup> Limelight Networks. "The State of Cybersecurity 2017 – Southeast Asia". 2018. Diakses pada 2 Agustus 2018. <https://www.limelight.com/resources/white-paper/state-of-cybersecurity-southeast-asia-2017/>

<sup>33</sup> Ibid.

<sup>34</sup> Margaret Rouse. TechTarget, Search Security. "Cybersecurity". Mei 2018. Diakses pada 6 November 2018. <https://searchsecurity.techtarget.com/definition/cybersecurity>

<sup>35</sup> Ibid.

<sup>36</sup> Ibid.

<sup>37</sup> Laurence Bradford. Forbes. "How to Start a Lucrative Career In Cybersecurity". 27 Februari 2017. Diakses pada 6 November 2018. <https://www.forbes.com/sites/laurencebradford/2017/02/27/how-to-start-a-lucrative-career-in-cybersecurity/#501d835d1066>

Berdasarkan uraian diatas, penulis menggunakan teori *The Organizational Readiness for Change* sebagai pisau analisis dalam tulisan ini. Teori ini dirumuskan oleh Bryan J. Weiner, seorang Profesor dari *Department of Global Health and Department of Health Services* pada *University of Washington*, Amerika Serikat.<sup>38</sup> Studi beliau berfokus pada implementasi, keberlanjutan dan inovasi pada sistem sebuah organisasi, khususnya organisasi yang melayani kesehatan publik dimana beliau mengajar.<sup>39</sup> Sebagaimana namanya, teori ini menjelaskan bagaimana kesiapan sebuah organisasi dalam menyikapi dan melakukan sebuah perubahan terhadap hal baru, pun begitu dengan seluruh elemen yang ada di dalamnya. Setiap unsur atau elemen di dalam organisasi itu bisa saling mempengaruhi satu sama lain terhadap perubahan atau revolusi yang dilakukan. Garis besar teori yang penulis gunakan ialah sebagai berikut.

“Organizational members shared resolve to implement a change (change commitment) and shared belief in their collective capability to do so (change efficacy)“. (BMC Implementation Science:2009).<sup>40</sup>

“How much organizational members value the change and how favorably they appraise?”. (BMC Implementation Science:2009).<sup>41</sup>

Teori ini membantu penulis menjelaskan bahwa “Readiness for Change” merujuk pada anggota dari organisasi tersebut dalam memiliki tekad yang sama untuk mengimplementasikan perubahan. Kutipan pernyataan yang pertama memiliki definisi bahwa anggota dari organisasi akan mengimplementasikan perubahan dengan mengubah komitmen hingga keyakinan yang sama dalam kapabilitas mereka masing masing (yang mampu mereka lakukan).<sup>42</sup> Kemudian, pernyataan yang kedua memiliki definisi bahwa bagaimana anggota organisasi tersebut dapat menilai bahwa perubahan itu berdampak baik atau tidak bagi mereka.<sup>43</sup> Bagaimana komitmen mereka serta kepercayaan diri atas kemampuan yang setiap anggota miliki sangat penting terhadap kemampuan organisasi tersebut untuk melakukan perubahan. Ketika kesiapan sebuah organisasi untuk berubah ini tinggi termasuk dengan unsur atau member di bawahnya

---

<sup>38</sup> University of Washington. Department of Global Health. Bryan J Weiner. About, Biography. 2018. Diakses pada 25 September 2018. <https://globalhealth.washington.edu/faculty/bryan-weiner>

<sup>39</sup> Ibid.

<sup>40</sup> Bryan Weiner. BMC, Implementation Science. A Theory of Organizational Readiness for Change. 19 Oktober 2009. Diakses pada 26 September 2018. <https://implementationscience.biomedcentral.com/articles/10.1186/1748-5908-4-67?report=reader>

<sup>41</sup> Ibid.

<sup>42</sup> Ibid.



juga tinggi, maka anggota organisasi tersebut akan mampu untuk mulai melakukan perubahan, mengerahkan usaha yang lebih besar, menunjukkan ketekunan yang lebih tinggi hingga memiliki sikap yang kooperatif.<sup>44</sup> Teori ini juga dapat mengukur perubahan dari organisasi dimana perilaku kolektif dibutuhkan secara efektif dalam mengimplementasikan suatu perubahan.<sup>45</sup> Pada landasan teori ini penulis akan memaparkan empat asumsi yang akan digunakan sebagai pisau analisa pada bagian analisis. Empat asumsi itu adalah sebagai berikut. Asumsi pertama yaitu “Organization” adalah organisasi regional di Asia Tenggara yaitu ASEAN. Asumsi kedua ialah “Member of Organization”, maksudnya adalah sepuluh negara yang menjadi anggota ASEAN. Lalu asumsi ketiga ialah “Implement to Change”, yaitu bagaimana setiap negara anggota ASEAN dapat mengimplementasikan perubahannya terhadap peningkatan sistem keamanan siber. Kemudian asumsi yang terakhir yaitu “Share believe in their collective capability”, maksudnya adalah negara-negara ASEAN saling berbagi keyakinan bahwa ancaman siber ini merupakan ancaman nyata yang perlu untuk dibuat sistem pertahanan siber sesuai dengan kemampuan negara masing-masing. Dengan pemaparan teori sekaligus dengan asumsi yang digunakan, maka penulis akan mengkaji bagaimana cara Singapura sebagai *Chair* ASEAN tahun 2018 memproyeksikan perubahan, yakni perubahan akan kesadaran negara – negara anggota ASEAN terhadap keamanan siber. Kesadaran ini akan mendorong suatu kebijakan negara untuk membangun infrastruktur di bidang keamanan siber yang sesuai dengan kapabilitas negara masing – masing.

## Analisis

Singapura sebagai *Chair* ASEAN memegang tanggung jawab untuk membawa ASEAN menjadi lebih baik sekaligus *adaptable* dan relevan dengan kondisi zaman saat ini. Secara garis besar kontribusi yang akan diberikan Singapura terhadap ASEAN pada 2018 ini tergambarkan pada naskah pidato Lee Hsien Loong pada saat agenda peresmian Singapura sebagai *Chairmanship* ASEAN 2018, pada 12 Januari 2018 lalu di Bishan-Ang Mio Kio

---

<sup>43</sup> Ibid.

<sup>44</sup> Bryan Weiner. University of Washington. ResearchGate. “A Theory of Organizational Readiness for Change”. Oktober 2009. Diakses pada 26 September 2018.

[https://www.researchgate.net/publication/38021465\\_A\\_theory\\_of\\_organizational\\_readiness\\_to\\_change](https://www.researchgate.net/publication/38021465_A_theory_of_organizational_readiness_to_change)

<sup>45</sup> Ibid.

Park, Singapura.<sup>46</sup> Pada inti pidato itu, Perdana Menteri Lee Hsien Loong menegaskan bahwa Singapura memiliki program untuk meningkatkan kekuatan kolektif negara-negara ASEAN. terhadap ancaman yang serius pada saat ini seperti Perubahan Iklim, Terorisme dan *Cybersecurity*.<sup>47</sup> *Cybersecurity* atau keamanan siber menjadi topik penelitian pada tulisan ini karena dianggap memiliki urgensi yang tinggi namun tidak dibarengi dengan langkah pencegahan atau pengamanan yang baik oleh negara-negara ASEAN. Selain itu, kawasan Asia Tenggara saat ini memang tengah bergulat dengan peningkatan ancaman siber yang signifikan, sehingga keamanan siber ini memang menjadi perhatian internasional khususnya perhatian bagi *Chair* ASEAN sendiri yang tiap tahunnya berganti.<sup>48</sup> Ancaman siber terus meningkat bagi negara-negara ASEAN karena memang mayoritas negaranya masih negara berkembang dan negara industri yang terdigitalisasi atau biasa disebut dengan Industri 4.0.<sup>49</sup>

Keamanan siber tergolong pada jenis keamanan non-tradisional yakni jenis keamanan yang baru menjadi isu keamanan pasca perang dingin usai, yaitu sekitar tahun 1990 an. Keamanan siber telah menjadi perhatian serius bagi hampir seluruh negara, sebab dunia saat ini mulai terdigitalisasi. Hampir semua sektor di dalam sistem kenegaraan telah masuk ke dalam dunia digital atau siber. Dunia siber ini disebut juga dengan *the fifth domain*.<sup>50</sup> *The Fifth Domain* atau domain kelima maksudnya ialah, internet atau siber merupakan medan peperangan kelima yang ada di dunia setelah empat medan peperangan lain yakni darat, laut, udara dan luar angkasa.<sup>51</sup> Hal itulah yang dimaksud bahwa hampir semua sektor di dalam negara telah terdigitalisasi, bukan hanya sektor pemerintahan saja, namun juga sektor ekonomi, perdagangan, keuangan, pendidikan, birokrasi, *database*, hingga sektor-sektor lainnya. Hal inilah yang kemudian menjadi alasan mengapa keamanan siber menjadi urgensi, karena ancaman siber memang nyata dan mengancam berbagai sektor yang telah terdigitalisasi. Dengan tingginya penggunaan internet di kawasan Asia Tenggara, seperti yang telah diuraikan pada landasan teori, negara – negara di Asia Tenggara akan memperoleh

---

<sup>46</sup> Association of Southeast Asia Nations. ASEAN Secretariat News. "PM Lee Hsien Loong Launches Singapore Chairmanship of ASEAN 2018 at the Experience ASEAN Carnival at Bishan-Ang Mo Kio Park. 13 Januari 2018. Diakses pada 26 September 2018. <https://asean.org/pm-lee-hsien-loong-launched-singapores-chairmanship-asean-2018-experience-asean-carnival-bishan-ang-mo-kio-park-12-january-2018/>

<sup>47</sup> Ibid.

<sup>48</sup> Prashanth Parameswaran. The Diplomat. "ASEAN Cybersecurity in the spotlight under Singapore's Chairmanship". 2 Mei 2018. Diakses pada 28 September 2018. <https://thediplomat.com/2018/05/asean-cybersecurity-in-the-spotlight-under-singapores-chairmanship/>

<sup>49</sup> Arief Subhan. The ASEAN Post. "Southeast Asia's Cybersecurity an Emerging Concern". 20 Mei 2018. Diakses pada 28 September 2018. <https://theaseanpost.com/article/southeast-asias-cybersecurity-emerging-concern>

<sup>50</sup> Matt Murphy. The Economist. "War In The Fifth Domain". 1 Juli 2010. Diakses pada 22 November 2018. <https://www.economist.com/briefing/2010/07/01/war-in-the-fifth-domain>

ancaman siber yang tinggi juga tentunya. Semakin banyak sektor dalam suatu negara yang terdigitalisasi, maka ancaman akan keamanan siber semakin tinggi karena akan menyerang sektor-sektor tersebut. Namun yang menjadi akar permasalahan ialah masih tingginya kerentanan negara – negara anggota ASEAN akan ancaman siber. Singapura sebagai *Chair ASEAN* mencoba untuk meningkatkan kesadaran negara anggota ASEAN terhadap keamanan siber melalui langkah yang dilakukan Singapura sendiri sebagai negara yang telah memiliki komitmen tinggi terhadap keamanan siber. Langkah yang dilakukan Singapura ini dapat penulis jelaskan dengan teori *Organizational Readiness for Change*. Sebagaimana telah dipaparkan pada bagian landasan teori, bahwa asumsi yang digunakan ialah ASEAN sebagai organisasi, *member of organization* adalah negara-negara anggota ASEAN. Kemudian *Implement to Change*, atau implementasi terhadap perubahan maksudnya adalah perubahan negara anggota-anggota ASEAN dalam rangka meningkatkan keamanan siber. Lalu yang terakhir ialah, *Shared believe in their collective capability*, atau saling memiliki keyakinan sesama negara ASEAN terhadap kemampuan masing masing dalam hal meningkatkan

---

<sup>51</sup> Ibid.

keamanan siber negara mereka. Jadi, Singapura sebagai pemimpin ASEAN di tahun 2018 ini berusaha untuk mengubah cara pandang negara lain terhadap keamanan siber, khususnya dalam ranah internasional, dikarenakan oleh urgensitasnya yang memang sudah tinggi. Dalam hal ini Singapura telah memberikan bukti bahwa negara tersebut memiliki komitmen tinggi terhadap pencegahan ancaman siber. Selain itu, Singapura juga telah membuktikan bahwa negara telah menerapkan atau memiliki sistem keamanan siber yang mumpuni. Jika mengambil ukuran dari seberapa besar negara menginvestasikan GDPnya untuk sektor keamanan siber, maka Singapura ada di urutan ketiga dari seluruh negara di dunia. Singapura berada di urutan ketiga dengan investasi sebesar 0,22% dari total *Gross Domestic Productnya*.<sup>52</sup> Dengan jumlah catatan investasi tersebut, Singapura berada dibawah peringkat dari Israel dan Inggris.<sup>53</sup> Sementara negara ASEAN lain yang menempati 10 besar hanyalah Malaysia yang menempati posisi ke-9 dengan menginvestasikan biaya sebesar 0,08% dari

---

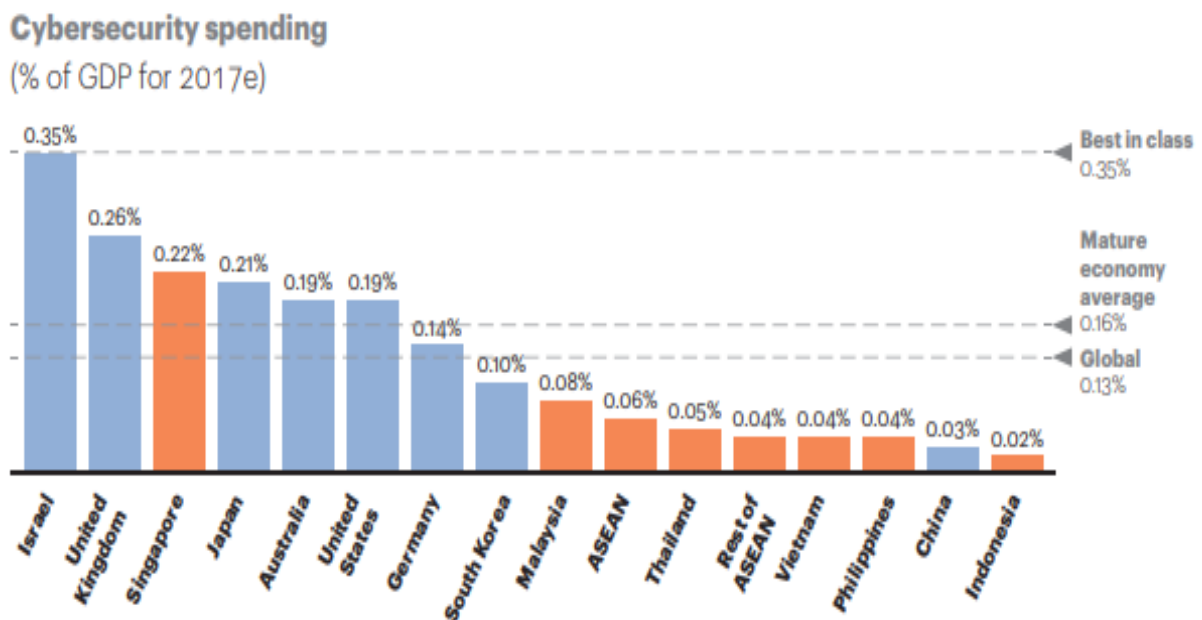
<sup>52</sup> Nikolai Dobberstein, Dieter Gerdemann, Gareth Pereira, Hoe Germaine. ATKearney. "Cybersecurity in ASEAN: An Urgent Call to Action". Diakses pada 28 September 2019. <http://www.southeast-asia.atkearney.com/documents/766402/15958324/Cybersecurity+in+ASEAN%E2%80%94An+Urgent+Call+to+Action.pdf/ffd3e1ef-d44a-ac3a-9729-22afbec39364>

<sup>53</sup> Ibid.

total *GDP*nya.<sup>54</sup> Masih pada sumber yang sama, jika keseluruhan negara ASEAN digabungkan dan dirata-ratakan. ASEAN hanya menempati urutan ke-10 sebagai organisasi negara yang mengalokasikan *GDP*nya untuk sektor keamanan siber yakni sebesar 0,05% dari keseluruhan *GDP* yang didapatkan ASEAN.<sup>55</sup> Data lebih lengkap telah tersaji pada grafik dibawah ini.

Data menunjukkan bahwa komitmen ASEAN terhadap keamanan siber belum menunjukkan angka yang baik. Karena dengan data yang penulis tampilkan, bahwa regional Asia Tenggara

Figure 7  
**Benchmarking cybersecurity spend as percent of GDP**



Note: Israel's cybersecurity spend benchmark is based on 2015 spend per capita.  
 Sources: Gartner; A.T. Kearney analysis

keseluruhan hanya menggunakan 0,06 % nya dari total *GDP* untuk meningkatkan keamanan sibernya.<sup>56</sup> Bila hal ini tidak segera ditingkatkan, ASEAN diprediksi akan mengalami kerugian sebesar 750 Miliar Dolar Amerika.<sup>57</sup> Ini menunjukkan bahwa kesadaran negara-

<sup>54</sup> Ibid.

<sup>55</sup> Ibid.

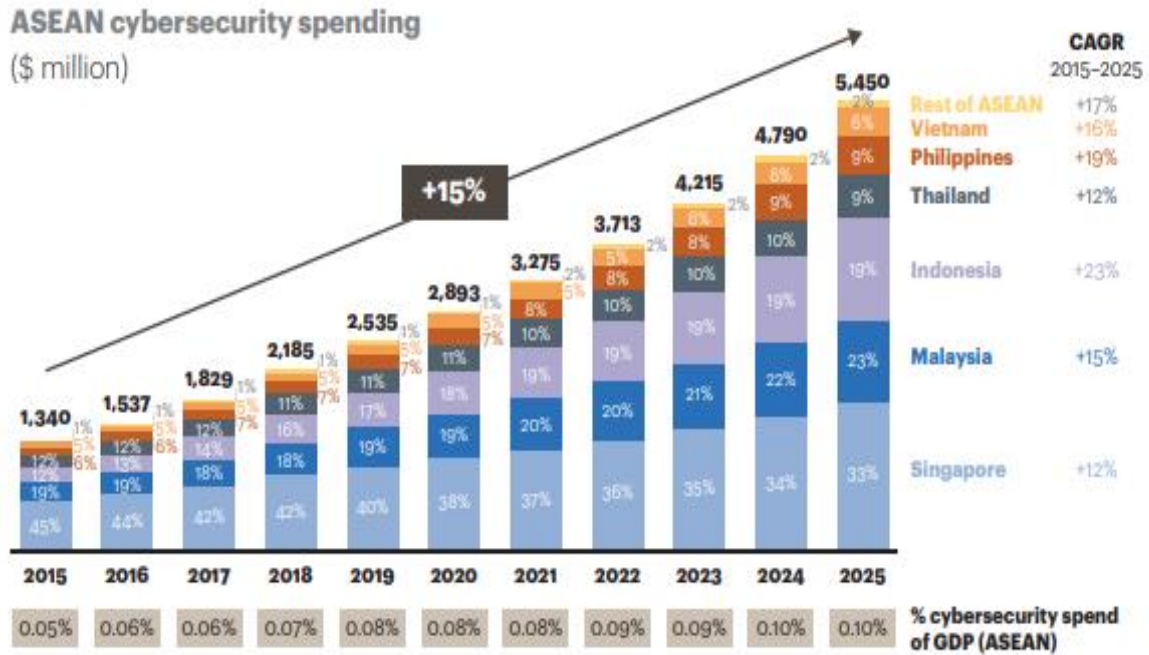
<sup>56</sup> Aqilah Allaudeen. Business Insider Singapore. "Singapore Leads ASEAN in its Cyber Security Policies, but The Region needs to work together: Report". 23 Januari 2018. Diakses pada 2 Agustus 2018. <https://www.businessinsider.sg/singapore-leads-asean-in-its-cyber-security-policies-but-the-region-needs-to-work-together-report/>

<sup>57</sup> Ibid.

negara anggota ASEAN masih kurang terkait ancaman siber. Mereka masih memiliki komitmen yang rendah terhadap keamanan siber negara masing masing. Tentunya permasalahan ini harus segera ditangani dan menemukan solusi yang tepat dan ideal. Seperti yang telah kita ketahui, pada tahun 2018 ini Singapura berkesempatan menjadi *Chair ASEAN*. Dengan posisi strategis ini, Singapura mencoba mengatasi permasalahan ini melalui program yang dicanangkannya yakni membangun keamanan kolektif negara anggota ASEAN dalam meningkatkan keamanan siber. Singapura mulai bergerak dalam rangka peningkatan keamanan siber. Langkah ini dimulai dengan menanamkan kesadaran terlebih dahulu kepada negara-negara anggota ASEAN bahwa ancaman siber memang benar adanya dan telah menjadi suatu ancaman non-tradisional yang nyata bagi dunia khususnya bagi negara-negara ASEAN. Ancaman ini akan mengancam kerentanan yang dimiliki setiap negara, dan menyebabkan bahaya yang akan berdampak pada sistem lain pada suatu negara, seperti ekonomi, perdagangan, keuangan, pemerintahan serta banyak sistem lain yang telah terdigitalisasi. Maka Singapura menyebarkan nilai-nilai perubahan bahwa negara-negara ASEAN sudah saatnya lebih sadar dan terbuka akan ancaman siber yang datang. Dengan nilai-nilai itu maka negara-negara anggota ASEAN akan lebih sadar dan peduli terhadap ancaman siber yang tak kasat mata namun jelas eksistensinya. Setelah adanya kesadaran dan kepedulian maka negara akan tergerak untuk mengembangkan sistem keamanan negaranya dalam menghadapi ancaman siber. Pada faktanya negara anggota ASEAN memiliki komitmen terhadap keamanan siber. Data selengkapnya tersaji pada grafik dibawah ini.

.

Figure 6  
**ASEAN cybersecurity spending is expected to show double-digit growth up to 2025**



Notes: Cybersecurity spend includes both private and public sector spend on the following: identity and access management, infrastructure protection (including content and endpoint), and network security.  
 Sources: International Data Corporation, Gartner; A.T. Kearney analysis

Dari data ini dapat kita simpulkan bahwa komitmen negara anggota ASEAN terhadap keamanan siber masih kurang. Hal ini memang bukan tanpa sebab, karena negara dengan kekuatan dan kestabilan politik ekonomi yang masih labil, cenderung akan mengutamakan pembangunan negaranya dalam sektor ekonomi, pendidikan, keamanan internal serta konflik etnis. Sedangkan, negara yang memang sudah maju dan memiliki situasi negara yang stabil serta kemajuan teknologinya yang sudah baik akan mengembangkan kapabilitas pertahanannya terhadap ancaman siber selain terhadap ancaman keamanan tradisional tentunya. Berbeda dengan negara berkembang atau negara yang belum memiliki kemitakhiran teknologi yang baik. Singapura –sebagai negara dari Asia Tenggara juga- telah menunjukkan bahwa negara ini memang benar memiliki komitmen yang tinggi terhadap keamanan siber. Bukti itu ditunjukkan dengan pemaparan data yang sebelumnya telah diuraikan dan ditampilkan bahwa Singapura menempati urutan ketiga diantara negara-negara di dunia. Hal ini sesungguhnya dapat meyakinkan negara-negara ASEAN bahwa Singapura yang memiliki program untuk meningkatkan kesadaran dan proteksi pada sistem pengamanan siber, bukan hanya program yang mengawang, namun sudah menjadi langkah nyata

setidaknya bagi Singapura sendiri. Pada grafik yang kedua, Singapura juga ditunjukkan sebagai negara yang memiliki komitmen dan proyeksi kuat kedepannya hingga tahun 2025 dalam komitmennya pada sistem keamanan siber. Sedangkan negara-negara anggota ASEAN yang lainnya berada di bawah Singapura. Pada penyajian data itu, Malaysia, Indonesia dan Thailand berada di bawah Singapura. Namun, dapat diprediksikan bahwa proyeksi komitmen negara tersebut terhadap keamanan siber meningkat tiap tahunnya, mengikuti jejak Singapura. Data itu mendukung argumentasi penulis bahwa pada tahun-tahun mendatang negara-negara ASEAN akan meningkatkan sistem keamanan sibernya, setelah menyadari adanya ancaman nyata dari serangan siber. Phillipina dan Vietnam berada pada posisi yang lebih rendah dengan angka yang cenderung meningkat juga secara perlahan pada prediksi tersebut. Sedangkan negara ASEAN yang lain berada di bawah Vietnam dengan angka yang lebih kecil. Dalam kasus ini, Singapura memimpin negara-negara ASEAN terkait kuatnya infrastruktur terhadap keamanan siber di ASEAN. Dengan menggunakan analisis teori *Organizational Readiness for Change* dapat dijelaskan bahwa Singapura sebagai negara yang paling berkomitmen terhadap keamanan siber dibanding negara ASEAN yang lainnya. Hal ini memiliki dampak sebagai penyebaran nilai bahwa keamanan siber merupakan hal yang penting, karena contohnya saja, Singapura sebagai negara ASEAN bisa menjadi negara yang tergolong kuat pengamanan sibernya. Selain itu menurut data dari *Global Cybersecurity Index*, Singapura juga termasuk ke dalam negara yang sudah *leading* dalam sistem pengaman sibernya bersama dengan Malaysia sebagai sesama negara dari Asia Tenggara.<sup>58</sup> Sedangkan negara Asia Tenggara lainnya hanya berada pada tahap *maturing* dan *initiating*.<sup>59</sup> Skala yang dibuat oleh *Global Cybersecurity Index* ini mengklasifikasikan negara-negara di dunia ke dalam 3 tingkatan terkait kapabilitas negaranya dalam membangun sistem pengamanan siber, yakni ada tingkatan *initiating*, *maturing* dan *leading*.<sup>60</sup> Pada tahap *initiating* terdapat 96 negara yang baru memulai komitmennya terhadap keamanan siber serta memiliki persentase dibawah 50% berdasarkan skala dari *Global Cybersecurity Index* tersebut.<sup>61</sup> pada tahap *maturing* terdapat 77 negara, yaitu tergolong ke dalam negara-negara yang sedang membangun sistem pertahanan sibernya lebih kompleks dan menginisiasi program – program baru dalam sektor keamanan siber dengan angka persentase antara 50 % – 80 % *Global*

---

<sup>58</sup> Brahima Sanou. International Telecommunication Union. “Global Cybersecurity Index”. 2017. Diakses pada 29 September 2018. [https://www.itu.int/dms\\_pub/itu-d/opb/str/D-STR-GCI.01-2017-PDF-E.pdf](https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2017-PDF-E.pdf)

<sup>59</sup> Ibid.

<sup>60</sup> Ibid.

<sup>61</sup> Ibid. Halaman 11.



*Security Index*.<sup>62</sup> Sedangkan pada tahap *leading* terdapat 21 negara dengan persentase diatas 80%, serta memiliki komitmen tinggi terhadap keamanan siber, hal inidibuktikan bahwa negara yang berada pada tahap *leading* telah mendemonstrasikan lima pilar pada *Global Cybersecurity Index*.<sup>63</sup> Selain tiga tingkatan itu, dalam metode penelitian yang kemudian menjadi dasar pengklarifikasian negara – negara di dunia, ada lima pilar yang menjadi indikator bagaimana sebuah negara telah memiliki komitmen pada sektor keamanan siber. Lima pilar tersebut adalah *legal*, *technical*, *organizational*, *capacity building* dan *cooperation*.<sup>64</sup> Pilar *legal* ini mengukur bagaimana eksistensi hukum yang berlaku di negara tersebut serta ketetapan lain yang berkaitan dengan legal konstitusi terhadap keamanan siber dan kejahatan siber.<sup>65</sup> Pilar *technical* mengukur bagaimana keberadaan lembaga teknis dan kerangka kerja pada sistem keamanan siber di suatu negara.<sup>66</sup> Pilar selanjutnya adalah *organizational*, yakni mengukur bagaimana koordinasi dari kebijakan antar institusi serta strategi pembangunan keamanan siber pada level nasional.<sup>67</sup> Pilar berikutnya ialah *capacity Building*, mengukur eksistensi dari penelitian dan pengembangan, pendidikan dan program pelatihan, sertifikasi bagi para profesional serta manajemen sektor publik pada aspek keamanan siber.<sup>68</sup> Pilar yang terakhir yaitu *cooperation*, yakni mengukur keberadaan kemitraan, kerangka kerja serta jaringan informasi bersama dalam keamanan siber.<sup>69</sup> Kelima pilar ini yang menjadi indikator *Global Cybersecurity Index* dalam menilai kapabilitas negara dalam keamanan siber. Dari penilaian tersebut, maka negara-negara diklasifikasikan pada tiga tingkatan yang telah penulis paparkan diatas. Berikut adalah tabel dari klasifikasi negara-negara di dunia, yang mana diantaranya terdapat negara anggota ASEAN. Negara anggota ASEAN tersebar pada tiga tahap atau tingkatan yang berbeda, berikut negara anggota ASEAN adalah yang diberi *highlight* berwarna kuning.

---

<sup>62</sup> Ibid. Halaman 11.

<sup>63</sup> Ibid. Halaman 11.

<sup>64</sup> Ibid. Halaman 4.

<sup>65</sup> Ibid. Halaman 4.

<sup>66</sup> Ibid. Halaman 4.

<sup>67</sup> Ibid. Halaman 4.

<sup>68</sup> Ibid. Halaman 4.

<sup>69</sup> Ibid. Halaman 4.

INITIATING		
Afghanistan	Guatemala	Palau
Andorra	Guinea	State of Palestine
Angola	Guinea-Bissau	Papua New Guinea
Antigua and Barbuda	Guyana	Saint Kitts and Nevis
Armenia	Haiti	Saint Lucia
Bahamas	Honduras	Saint Vincent & the Grenadines
Barbados	Iraq	Samoa
Belize	Jordan	San Marino
Benin	Kiribati	Sao Tome and Principe
Bhutan	Kuwait	Seychelles
Bolivia (Plurinational State of)	Kyrgyzstan	Sierra Leone
Bosnia & Herzegovina	Lebanon	Solomon Islands
Burkina Faso	Lesotho	Somalia
Burundi	Liberia	South Sudan
<b>Cambodia</b>	Libya	Sudan
Cape Verde	Liechtenstein	Suriname
Central African Republic.	Madagascar	Swaziland
Chad	Malawi	Syrian Arab Republic
Comoros	Maldives	Tajikistan
Congo	Mali	Timor-Leste
Cuba	Marshall Islands	Togo
Democratic Republic of the Congo	Mauritania	Tonga
Djibouti	Micronesia	Trinidad and Tobago
Dominica	Monaco	Turkmenistan
Dominican Republic	Mongolia	Tuvalu
El Salvador	Mozambique	Uzbekistan
Equatorial Guinea	<b>Myanmar</b>	Vanuatu
Eritrea	Namibia	Vatican
Ethiopia	Nauru	<b>Viet Nam</b>
Fiji	Nepal (Republic of)	Yemen
Gabon	Nicaragua	Zambia
Gambia	Niger	Zimbabwe
Grenada		

MATURING		
Albania	Ghana	Peru
Algeria	Greece	Philippines
Argentina	Hungary	Poland
Austria	Iceland	Portugal
Azerbaijan	India	Qatar
Bahrain	Indonesia	Romania
Bangladesh	Iran (Islamic Republic of)	Rwanda
Belarus	Ireland	Saudi Arabia
Belgium	Israel	Senegal
Botswana	Italy	Serbia
Brazil	Jamaica	Slovakia
Brunei Darussalam	Kazakhstan	Slovenia
Bulgaria	Kenya	South Africa
Cameroon	Laos	Spain
Chile	Latvia	Sri Lanka
China	Lithuania	Tanzania
Colombia	Luxembourg	Thailand
Costa Rica	Malta	The Former Yugoslav Rep. of Macedonia
Côte d'Ivoire	Mexico	Tunisia
Croatia	Moldova	Turkey
Cyprus	Montenegro	Uganda
Czech Republic	Morocco	Ukraine
Dem. People's Rep. of Korea	Nigeria	United Arab Emirates
Denmark	Pakistan	Uruguay
Ecuador	Panama	Venezuela
Germany	Paraguay	

LEADING		
Australia	Japan	Oman
Canada	Korea	Russian Federation
Egypt	Malaysia	Singapore
Estonia	Mauritius	Sweden
Finland	Netherlands	Switzerland
France	New Zealand	United Kingdom
Georgia	Norway	United States

Dalam skala yang dibuat oleh *Global Cybersecurity Index* ini juga menunjukkan bahwa Singapura memimpin dalam sistem keamanan siber, bukan hanya bagi negara anggota ASEAN, namun juga dalam lingkup internasional, seperti tergambar pada grafik maupun tertera pada tabel diatas. Singapura dan Malaysia tergolong pada kelompok negara yang sudah *leading*. Brunei Darussalam, Indonesia, Laos, Filipina dan Thailand berada pada tingkatan *maturing*. Sedangkan Kamboja, Vietnam dan Myanmar masih pada tahapan *initiating*. Dalam analisis ini, Singapura sebagai negara yang sudah memiliki kapabilitas yang

mumpuni dalam pencegahan kejahatan siber, dapat memberikan nilai positif bagi negara-negara ASEAN lainnya, bahwa memiliki sistem keamanan siber adalah hal yang *urgent* dan ideal untuk diwujudkan. Fakta ini dapat dijadikan model untuk proyeksi pembangunan sistem pertahanan siber bagi negara-negara ASEAN. Bila kita melihat data statistik berdasarkan indeks dari *Global Cybersecurity Index*, Singapura menempati posisi teratas dengan rata rata indeks tertinggi diatas Amerika Serikat, dengan poin 0,92. Angka ini diperoleh dari penghitungan rata-rata poin dari kelima pilar *cybersecurity* yang dimiliki oleh tiap negara. Kelima poin dari pilar *cybersecurity* ini dijumlahkan lalu dibagi jumlah pilar *Global Cybersecurity Index*, sehingga angka itulah yang dinamakan *GCI Score*, yang kemudian menjadi penentu berada pada peringkat berapakah suatu negara. Berikut adalah rumus penghitungan *GCI* untuk suatu negara.<sup>70</sup>

Score

$$Me = \frac{\sum xi}{n} \qquad Me = \frac{L+T+O+Cb+C}{n}$$

<sup>70</sup> Diadaptasi dari rumus penghitungan mean atau rata-rata pada buku “Statistika Untuk Penelitian”. Bab 2. Halaman 49-50. Karya Sugiyono. Alfabeta. Bandung. Maret 2016. ISBN: 978-979-8433-10-8

- |    |                         |    |                                |
|----|-------------------------|----|--------------------------------|
| Me | = Rata-rata = GCI Score | Cb | = Capacity Building            |
| L  | = Legal                 | C  | = Cooperation                  |
| T  | = Technical             | n  | = 5 (Jumlah pilar <i>GCI</i> ) |
| O  | = Organizational        |    |                                |

Fakta tersebut membuktikan bahwa Singapura bukan hanya menjadi negara yang terkuat sistem keamanan sibernya di Asia Tenggara, melainkan juga di dunia menjadi nomor satu. Singapura memang memiliki sistem pengendalian terpusat dalam sektor kejahatan atau insiden siber, sistem ini lebih baik dari Amerika Serikat serta negara – negara potensial lain di dunia.<sup>71</sup> Sedangkan negara ASEAN lainnya yaitu Malaysia berada pada posisi ketiga di bawah Amerika Serikat. Untuk urutan negara selengkapnya dapat dilihat pada tabel di bawah ini.

<sup>71</sup> Kevin Kwang. Channel News Asia. “Singapore Can Play ‘Important role’ In Cybersecurity for SEA Region, say FireEye CEO”. 5 Oktober 2018. Diakses pada 11 November 2018.  
<https://www.channelnewsasia.com/news/technology/singapore-can-play-important-role-in-cybersecurity-for-sea-10793700>

**Table 5.1: Top ten most committed countries, GCI (normalized score)**

Country	GCI Score	Legal	Technical	Organizational	Capacity Building	Cooperation
Singapore	0.92	0.95	0.96	0.88	0.97	0.87
United States	0.91	1	0.96	0.92	1	0.73
Malaysia	0.89	0.87	0.96	0.77	1	0.87
Oman	0.87	0.98	0.82	0.85	0.95	0.75
Estonia	0.84	0.99	0.82	0.85	0.94	0.64
Mauritius	0.82	0.85	0.96	0.74	0.91	0.70
Australia	0.82	0.94	0.96	0.86	0.94	0.44
Georgia	0.81	0.91	0.77	0.82	0.90	0.70
France	0.81	0.94	0.96	0.60	1	0.61
Canada	0.81	0.94	0.93	0.71	0.82	0.70

Dengan tampilan data pada tabel diatas, maka Singapura dapat lebih memberikan pengaruhnya terhadap negara-negara anggota ASEAN terkait langkahnya dalam meningkatkan keamanan siber. Berdasarkan pemaparan tersebut, Singapura telah menandakan negaranya sebagai negara yang paling mumpuni dalam sistem keamanan siber di dunia. Dengan pencapaian itu, tidak heran jika Singapura memiliki program untuk meningkatkan keamanan siber di Asia Tenggara melalui negara-negara anggota ASEAN. Singapura berupaya untuk memberikan keyakinan kepada seluruh negara ASEAN untuk bersama-sama membangun sistem pertahanan sibernya. Bagaikan gayung bersambut, kesepuluh negara ASEAN setuju untuk membuat kerangka kerja formal terkait keamanan, kebijakan hingga operasional sistem keamanan siber untuk regional Asia Tenggara.<sup>72</sup> Kesepakatan ini dibuat pada *ASEAN Ministerial Conference on Cybersecurity* pada 19 September 2018 ini, dan Singapura lah yang diberi mandat untuk membuat proposal kerangka kerja ini untuk kemudian menjadi bahan pertimbangan negara-negara anggota ASEAN.<sup>73</sup> Melalui AMCC, esepuluh negara ASEAN sepakat untuk meningkatkan keamanan

<sup>72</sup> Eilen Yu. ZDNet. "ASEAN Countries to Established Framework for Cybersecurity Collaboration." 20 September 2018. Diakses pada 10 November 2018. <https://www.zdnet.com/article/asean-countries-to-establish-framework-for-cybersecurity-collaboration/>

<sup>73</sup> Ibid.

siber, sebab sektor ini sangat mendukung kemajuan ekonomi dan perbaikan standar hidup.<sup>74</sup> Namun kembali lagi bahwa norma perilaku tiap negara bersifat sukarela dan tidak mengikat, tetapi langkah-langkah membangun kepercayaan antar negara tetaplah merupakan hal yang esensial bagi stabilitas regional khususnya dalam hal ini terkait isu *cybersecurity*.<sup>75</sup> Pernyataan ini dirilis langsung oleh *Cyber Security Agencies of Singapore*. Pernyataan serupa juga diutarakan oleh Menteri Komunikasi dan Informasi Singapura, S Iswaran. Beliau mengatakan bahwa “Singapura dan seluruh negara ASEAN membutuhkan lingkungan *cybersecurity* berbasis aturan yang jelas, untuk mendukung terjalinnya hubungan yang baik serta rasa saling percaya antar negara anggota”<sup>76</sup> Apa yang dilakukan Singapura ini telah memiliki dampak pada ketersediaan negara ASEAN lain untuk memperkuat keamanan sibernya, bukan hanya pada level nasional, namun juga pada level regional, ditandai dengan digagasnya kerangka kerjasama keamanan siber level ASEAN tersebut. Jika penulis refleksi pada teori yang digunakan, Singapura sebagai aktor kunci dari “Readiness for Change” ini memang memiliki dampak bagi negara ASEAN lainnya. Singapura mengakomodir perubahan dalam peningkatan sistem keamanan siber. Singapura juga telah menunjukkan secara implisit bahwa negara ASEAN pun mampu memiliki sistem pertahanan siber yang kuat. Apa yang telah diselenggarakan Singapura ini sedikitnya telah mengimplementasikan program Singapura sebagai *Chair ASEAN 2018* ini. Sebagai *Chair ASEAN 2018* ini, Singapura telah mendorong terselenggaranya banyak agenda terkait keamanan siber, investasi sumber daya yang besar dalam membangun sistem operasional, kebijakan, serta kapasitas ketahanan siber dalam level regional.<sup>77</sup> Sebagaimana dengan topik besar pada program yang dibawa oleh Singapura ketika menjadi *Chair ASEAN –Innovation and Resilience-* negara dengan tingkat kemajuan teknologi terbaik memiliki tanggung jawab untuk mensosialisasikan nilai dan norma baru, landasan hukum internasional, hingga perilaku negara yang baik dan bertanggung jawab dalam dunia siber.<sup>78</sup> Singapura juga membangun beberapa lembaga negara terkait keamanan siber. Seperti *Cyber Think Tank and Training Centre, Cyber Range Training Centre* dan *Computer Emergency Response Team (CERT)*

---

<sup>74</sup> Cyber Security Agency of Singapore. Press Release: “ASEAN Member States Agree to Strengthen Cyber Coordination and Capacity Building Efforts.” 19 September 2018. Diakses pada 9 November 2018.

<https://www.csa.gov.sg/news/press-releases/amcc-2018>

<sup>75</sup> Ibid.

<sup>76</sup> Hariz Baharudin. The Strait Times. Singapore. “ASEAN Framework on Cyber Security in The Works”. 20 September 2018. Diakses pada 10 November 2018. <https://www.straitstimes.com/singapore/asean-framework-on-cyber-security-in-the-works>

<sup>77</sup> Elina Noor. The Diplomat. “ASEAN Takes a Bold Cybersecurity Step.” 4 Oktober 2018. Diakses pada 10 November 2018. <https://thediplomat.com/2018/10/asean-takes-a-bold-cybersecurity-step/>

<sup>78</sup> Ibid.

*Centre*.<sup>79</sup> Untuk kebutuhan ini, Singapura telah mengucurkan dana segar sejumlah 30 juta Dollar Singapura.<sup>80</sup> Sesungguhnya, Singapura tidak hanya menanamkan eksistensinya sebagai negara yang *concern* terhadap keamanan siber di ASEAN, namun juga di dunia. Salah satu buktinya adalah fakta bahwa Singapura merupakan negara dengan sistem keamanan siber terbaik di dunia menurut laporan dari *Global Cybersecurity Index*. Kemudian, pada tanggal 1-3 Juni lalu, Singapura menjadi penyelenggara *International Institute of Strategic Studies, Shangri-la Dialogue* di Hotel Shangri-la, Singapura.<sup>81</sup> *IISS Shangri-la dialogue* ini membahas mengenai isu keamanan dan *strategic affairs* di Asia Pasifik termasuk di dalamnya juga membahas isu keamanan siber.<sup>82</sup> Pada agenda tersebut Perdana Menteri India Narendra Modi dan Sekretaris bidang Pertahanan Amerika Serikat, James Mattis berkesempatan menjadi *Keynote Speaker*.<sup>83</sup> Secara umum mereka membahas mengenai kemitraan strategis serta peran negara India dan Amerika sendiri dalam regional Asia Pasifik.<sup>84</sup> Dipilihnya Singapura sebagai tuan rumah dari *IISS Shangri-la dialogue* ini tentunya menambah citra Singapura sebagai negara yang strategis terkait isu keamanan dan kajian strategis. Tidak hanya itu, terpilih ‘negeri singa’ sebagai tuan rumah juga menambah *bargaining point* Singapura sebagai negara yang memiliki komitmen tinggi terhadap sektor keamanan khususnya keamanan siber. Terlebih lagi Singapura di regionalnya sendiri yakni Asia Tenggara sedang menjadi pemimpin ASEAN, yang sedang melaksanakan program pembangunan ketahanan regional dalam sektor keamanan siber. Selain diselenggarakannya *IISS Shangri-la dialogue*, Singapura juga melakukan kerjasama dengan beberapa aktor non-regional, diantaranya pada bulan Oktober lalu, Singapura, Indonesia dan Australia menyelenggarakan agenda *ASEAN Cyber Security Mission 2018* di *Singapore Cloud and Cyber Security Expo* di Singapura serta pada *The Indonesia Cyber Security Summit* di Bali pada tanggal 10-19 Oktober 2018 lalu.<sup>85</sup> Kemudian pada pertengahan November lalu,

---

<sup>79</sup> Channel News Asia. “Singapore to Pump In S\$ 30m for New Regional Cybersecurity Training Centre”. 19 September 2018. Diakses pada 11 November 2018.

<https://www.channelnewsasia.com/news/singapore/singapore-to-pump-in-s-30m-for-new-regional-cybersecurity-10735308>

<sup>80</sup> Ibid.

<sup>81</sup> Info selengkapnya dapat dilihat di “IISS Cyber Report: 1 to 7 June”. 7 Juni 2018. Diakses pada 11 November 2018. <https://www.iiss.org/blogs/cyber-report/2018/06/1-to-7-june>

<sup>82</sup> Ibid.

<sup>83</sup> Ibid.

<sup>84</sup> Ibid.

<sup>85</sup> Australian Government, Australian Trade and Investment Commission. Australia Unlimited. “ASEAN Cyber Security Mission Summit 2018”. 2018. Diakses pada 6 Desember 2018.

<https://www.austrade.gov.au/EventViewBookingDetails.aspx?Bck=Y&EventID=25389&m=0|0#/event>.

Singapura telah menyepakati kerjasama di bidang *cybersecurity* dengan Amerika Serikat.<sup>86</sup> Kesepakatan kerjasama antara Singapura dengan Amerika Serikat ini berfokus pada *Cybersecurity Technical Assistance* antar kedua negara dengan sasaran untuk negara anggota ASEAN.<sup>87</sup> Lebih jauh lagi, kerjasama ini akan melakukan penguatan pada kapasitas regional Asia Tenggara terhadap sistem keamanan siber.<sup>88</sup> Selain dengan Amerika Serikat, sebelumnya Singapura juga telah menekan kerjasama pada bidang keamanan siber dengan negara Amerika Utara lain yaitu Kanada.<sup>89</sup> Dalam kerjasama ini, baik Singapura dan Kanada menyepakati adanya pertukaran informasi dari segi ancaman dan serangan siber, saling melakukan pelatihan terhadap sumber daya manusia, pengembangan standardisasi keamanan siber, ketentuan teknis, sertifikasi hingga pengembangan kapasitas keamanan siber regional.<sup>90</sup> Selain kedua negara tersebut, Singapura telah menekan kerjasama juga sebelumnya dengan negara Asia Timur yaitu Jepang. Pada tahun 2017 lalu, David Koh, mewakili *Singapore's Cyber Security Agency*, serta Ikuo Misomi selaku perwakilan dari *Japan's National Center of Incident Readiness and Strategy for Cybersecurity*, menekan kesepakatan dalam bidang keamanan siber.<sup>91</sup> Melalui kesepakatan ini, langkah-langkah yang dilakukan ialah pertukaran informasi, peningkatan kesadaran terkait *cybersecurity*, hingga pertukaran tenaga ahli.<sup>92</sup> Pada september lalu, ASEAN dan Jepang telah melaksanakan *ASEAN-Japan Cybersecurity Capacity Building Center* di Bangkok.<sup>93</sup> Program ini merupakan *workshop* keamanan siber yang diselenggarakan oleh ASEAN bekerja sama dengan Jepang. Dalam *workshop* ini Jepang berbagi pengalaman dan keahlian dalam mengidentifikasi dan bertahan dari serangan siber.<sup>94</sup> Selain bekerja sama dengan negara lain non-ASEAN, Singapura juga melakukan kerjasama dengan pihak swasta yang khusus bergerak di bidang *cybersecurity*. Langkah ini dilakukan sebab, ancaman siber sesungguhnya bukan hanya datang dari aktor negara saja, namun aktor

---

<sup>86</sup> Channel News Asia. "US Singapore to Collaborate on Cybersecurity for ASEAN". 16 November 2018. Diakses pada 6 Desember 2018. <https://www.channelnewsasia.com/news/singapore/cybersecurity-asean-us-singapore-work-together-10936910>

<sup>87</sup> Ibid.

<sup>88</sup> Ibid.

<sup>89</sup> Channel News Asia. "Singapore, Canada Agree to Boost Cybersecurity Cooperation". 14 November 2018. Diakses pada 5 Desember 2018. [https://www.channelnewsasia.com/news/singapore/singapore-canada-cybersecurity-cooperation-mou-agreement-10930094?cid=h3\\_referral\\_inarticlelinks\\_24082018\\_cna](https://www.channelnewsasia.com/news/singapore/singapore-canada-cybersecurity-cooperation-mou-agreement-10930094?cid=h3_referral_inarticlelinks_24082018_cna)

<sup>90</sup> Ibid.

<sup>91</sup> Kyodo. The Japan Times. "Singapore and Japan Ink Accord to Strengthen Cybersecurity Cooperation." 19 September 2017. Diakses pada 7 Desember 2018. <https://www.japantimes.co.jp/news/2017/09/19/national/singapore-japan-ink-accord-strengthen-cybersecurity-cooperation/#.XAqOmgzblU>

<sup>92</sup> Ibid.

<sup>93</sup> Hiroshi Kotani. Nikkei Asian Review. "Southeast Asia Boosts Cybersecurity Training With Bangkok Center". 14 September 2018. Diakses pada 9 Desember 2018. <https://asia.nikkei.com/Politics/International-Relations/Southeast-Asia-boosts-cybersecurity-training-with-Bangkok-center>



non-negara bahkan individu juga bisa menjadi ancaman yang patut diperhitungkan. Dengan demikian, usaha untuk pencegahan dari serangan siber juga harus melibatkan pihak swasta yang memang ahli dalam bidangnya. Singapura telah banyak melakukan kerjasama dengan *cybersecurity* company itu, salah satunya adalah kerjasama dengan “CyLon”, lembaga swasta asal inggris yang berfokus pada pembangunan sistem keamanan siber.<sup>95</sup>

## Kesimpulan

Singapura sebagai *Chair* ASEAN memiliki program “Resillience and Innovation” untuk meningkatkan kapabilitas negara di ASEAN dalam keamanan kolektifnya terhadap ancaman kontemporer yang berupa pemanasan global, terorisme dan keamanan siber. Keamanan siber memang menjadi isu yang sedang menjadi perhatian dunia internasional, namun tidak bagi negara berkembang, karena negara cenderung menaruh perhatiannya pada isu keamanan lain. Namun, Singapura sebagai negara yang berasal dari regional yang didominasi negara berkembang memandang bahwa ancaman siber tetaplah merupakan ancaman yang perlu mendapatkan perhatian khusus. Sikap ini dibuktikan dengan langkah yang telah dilakukan Singapura dalam melakukan pembangunan pertahanan negara terhadap pencegahan dari ancaman siber. Kemudian Singapura juga melakukan kerjasama *workshop* di bidang *cybersecurity*, membangun kerjasama dengan negara maupun aktor non-negara yang dalam hal ini pihak swasta yang memang bergerak di bidang keamanan siber, hingga menjadi tuan rumah dari agenda seminar internasional mengenai *cybersecurity*. Selain itu, Singapura juga tergolong ke dalam negara yang sudah *leading* dalam sistem keamanan sibernya menurut data dari *Global Cybersecurity Index*. Maka, langkah-langkah yang telah dijalankan Singapura tersebut, sudah menjawab pertanyaan penelitian yang telah penulis utarakan pada bagian rumusan masalah di atas. Dengan pencapaian ini, negara–negara ASEAN lain diharapkan dapat melihat bagaimana negara Singapura telah mampu membangun kekuatan pertahanan sibernya, dan memberikan kesamaan nilai dan keyakinan bagi negara ASEAN lainnya.

Sampai tulisan ini dibuat hingga naik cetak, Singapura masih menjadi *Chair* ASEAN 2018. Pada masa yang akan datang, sangat mungkin untuk dilakukan penelitian lebih lanjut dan

---

<sup>94</sup> Ibid.

<sup>95</sup> Nicky Lung, OpenGov Asia. “How Cyber Security Agency is Protecting Singapore In The Changing Cyber Landscape”. 1 April 2018. Diakses pada 8 Desember 2018. <https://www.opengovasia.com/how-cyber-security-agency-is-protecting-singapore-in-the-changing-cyber-landscape/>

mendalam terkait apa saja peran yang telah dilakukan Singapura sebagai *Chair* ASEAN pada tahun 2018, khususnya pada aspek *cybersecurity*. Bagaimana dampak dan pengaruhnya terhadap dinamika ASEAN untuk lima hingga sepuluh tahun mendatang.

## Daftar Pustaka

- Abdurashitov, Oleg. KasperskyLab. "ASEAN Cyber Diplomacy: Overcoming Differences". 30 Oktober 2018. Diakses pada 7 Desember 2018. <https://www.kaspersky.com/about/policy-blog/general-cybersecurity/asean-cyber-diplomacy-overcoming-differences>
- "32nd ASEAN Summit – Chairman Statement". ASEAN Singapore 2018. Resilient and Innovative, Press Release. 28 April 2018. Diakses pada 20 Juli 2018. [https://www.asean2018.sg/Newsroom/Press-Releases/Press-Release-Details/20180428\\_Chairmans\\_Statement](https://www.asean2018.sg/Newsroom/Press-Releases/Press-Release-Details/20180428_Chairmans_Statement)
- "South Eastern Asia Population". Worldometers. 20 Juli 2018. Diakses pada 20 Juli 2018. <http://www.worldometers.info/world-population/south-eastern-asia-population/>
- Allaudeen, Aqilah. Bussiness Insider Singapore. "Singapore Leads ASEAN in its Cyber Security Policies, but The Region needs to work together: Report". 23 Januari 2018. Diakses pada 2 Agustus 2018. <https://www.businessinsider.sg/singapore-leads-asean-in-its-cyber-security-policies-but-the-region-needs-to-work-together-report/>
- Australian Government, Austalian Trade and Investment Commission. Australia Unilimited. "ASEAN Cyber Security Mission Summit 2018". 2018. Diakses pada 6 November 2018. <https://www.austrade.gov.au/EventViewBookingDetails.aspx?Bck=Y&EventID=25389&m=0|0#/event>
- ASEAN Singapore 2018. Resilient and inovative. "Experience ASEAN Festival – Opening Remarks by Prime Minister Lee Hsien Loong". 13 Januari 2018. Diakses pada 31 Juli 2018. <https://www.asean2018.sg/MFA/Newsroom/Press-Releases/Press-Release-Details/20180112>
- Association of Southeast Asia Nations. ASEAN Secretariat News. "PM Lee Hsien Loong Launches Singapore Chairmanship of ASEAN 2018 at the Experience ASEAN Carnival at Bishan-Ang Mo Kio Park. 13 Januari 2018. Diakses pada 26 September 2018. <https://asean.org/pm-lee-hsien-loong-launched-singapores-chairmanship-asean-2018-experience-asean-carnival-bishan-ang-mo-kio-park-12-january-2018/>
- Association of Southeast Asia Nations. ASEAN Secretariat News. "PM Lee Hsien Loong Launches Singapore Chairmanship of ASEAN 2018 at the Experience ASEAN Carnival at Bishan-Ang Mo Kio Park. 13 Januari 2018. Diakses pada 26 September 2018. <https://asean.org/pm-lee-hsien-loong-launched-singapores-chairmanship-asean-2018-experience-asean-carnival-bishan-ang-mo-kio-park-12-january-2018/>
- Baharudin, Hariz. The Strait Times. Singapore. "ASEAN Framework on Cyber Security in The Works". 20 September 2018. Diakses pada 10 November 2018. <https://www.straittimes.com/singapore/asean-framework-on-cyber-security-in-the-works>
- Brandon, John. The Asia Foundation. "Why ASEAN Needs to Invest More In Cybersecurity". 9 Mei 2018. Diakses pada 8 Desember 2018. <https://asiafoundation.org/2018/05/09/why-asean-needs-to-invest-more-in-cybersecurity/>

Cyber Security Agency of Singapore. Press Release: "ASEAN Member States Agree to Strengthen Cyber Coordination and Capacity Building Efforts." 19 September 2018. Diakses pada 9 November 2018. <https://www.csa.gov.sg/news/press-releases/amcc-2018>

Channel News Asia. "Singapore to Pump In S\$ 30m for New Regional Cybersecurity Training Centre". 19 September 2018. Diakses pada 11 November 2018. <https://www.channelnewsasia.com/news/singapore/singapore-to-pump-in-s-30m-for-new-regional-cybersecurity-10735308>

Channel News Asia. "Singapore, Canada Agree to Boost Cybersecurity Cooperation". 14 November 2018. Diakses pada 5 Desember 2018. [https://www.channelnewsasia.com/news/singapore/singapore-canada-cybersecurity-cooperation-mou-agreement-10930094?cid=h3\\_referral\\_inarticlelinks\\_24082018\\_cna](https://www.channelnewsasia.com/news/singapore/singapore-canada-cybersecurity-cooperation-mou-agreement-10930094?cid=h3_referral_inarticlelinks_24082018_cna)

Channel News Asia. "US Singapore to Collaborate on Cybersecurity for ASEAN". 16 November 2018. Diakses pada 6 Desember 2018. <https://www.channelnewsasia.com/news/singapore/cybersecurity-asean-us-singapore-work-together-10936910>

Daniel, "Southeast Asia Internet Users are Booming". PPC Land. 4 Mei 2018. Diakses pada 20 Juli 2018. <https://ppc.land/southeast-asia-internet-users-are-booming/>

Dobberstein, Nikolai., Dieter Gerdemann, Gareth Pereira, Hoe Germaine. ATKearney. "Cybersecurity in ASEAN: An Urgent Call to Action". Diakses pada 28 September 2019. <http://www.southeast-asia.atkearney.com/documents/766402/15958324/Cybersecurity+in+ASEAN%E2%80%94%94An+Urgent+Call+to+Action.pdf/ffd3e1ef-d44a-ac3a-9729-22afbec39364> DOI 10.1007/978-1-4614-7205-6

Elina Noor. The Diplomat. "ASEAN Takes a Bold Cybersecurity Step." 4 Oktober 2018. Diakses pada 10 November 2018. <https://thediplomat.com/2018/10/asean-takes-a-bold-cybersecurity-step/>

Fernando, Donny. The Jakarta Post. "Indonesia Records \$4,8 Billion in Digital Economy". 13 Januari 2018. Diakses pada 30 Juli 2018. <http://www.thejakartapost.com/news/2018/01/31/indonesia-records-4-8-billion-investment-in-digital-economy.html>

Fifth Domain. What is Fifth Domain?. 2018. Diakses pada 26 September 2018. <https://www.fifthdomain.com/about-us/>

Hollander, Rayna. Business Insider. "Southeast Asia Could be a Leader in Mobile Internet User Next Year". 13 Desember 2017. Diakses pada 20 Juli 2018. <http://www.businessinsider.com/southeast-asia-could-be-a-leader-in-mobile-internet-usage-next-year-2017-12/?IR=T>

- Ignatuschtschenko, Eva. "Developing a Cyber Harm Model". Global Cyber Security Capacity Centre. Oxford Martin School. University of Oxford. 12 Januari 2016. Diakses pada 9 Desember 2018. [Sci-hub.se/https://www.sbs.ox.ac.uk/cybersecurity-capacity/system/files/EIgnatuschtschenko\\_GCSCC\\_presentation\\_160112\\_0.pdf](https://www.sbs.ox.ac.uk/cybersecurity-capacity/system/files/EIgnatuschtschenko_GCSCC_presentation_160112_0.pdf)
- International Institute of Strategic Studies. IISS Cyber Report: 1 to 7 June 2018. 17th IISS Shangri – La Dialogue Highlights Indo – Pacific Concern. 7 Juni 2018. Diakses pada 11 November 2018. <https://www.iiss.org/blogs/cyber-report/2018/06/1-to-7-june>
- Justina Lee. Business Trend, Nikkei, Asian Review "ASEAN Remains "Prime Target" for Cyberattacks". 8 Februari 2018. Diakses pada 20 Juli 2018. <https://asia.nikkei.com/Business/Business-Trends/ASEAN-remains-prime-target-for-cyberattacks>
- Kazakova, Anastasiya. KasperskyLab. "What's To Be Done About The Militarization of Cyberspace? More Cooperation With Each Other". 30 Oktober 2018. Diakses pada 6 Desember 2018. <https://www.kaspersky.com/about/policy-blog/general-cybersecurity/how-to-deal-with-militarizing-cyberspace>
- Kemp, Simon. Hootsuite. We Are Social. TechInAsia. "The Full Guide to Southeast Asia Digital Landscpe in 2017". 8 Februari 2017. Diakses pada 2 Agustus 2018. <https://www.techinasia.com/talk/full-guide-southeast-asia-digital-landscape-2017>
- Kotani, Hiroshi. Nikkei Asian Review. "Southeast Asia Boosts Cybersecurity Training With Bangkok Center". 14 September 2018. Diakses pada 9 Desember 2018. <https://asia.nikkei.com/Politics/International-Relations/Southeast-Asia-boosts-cybersecurity-training-with-Bangkok-center>
- Kwang, Kevin. Channel News Asia. "Singapore Can Play 'Important role' In Cybersecurity for SEA Region, say FireEye CEO". 5 Oktober 2018. Diakses pada 11 November 2018. <https://www.channelnewsasia.com/news/technology/singapore-can-play-important-role-in-cybersecurity-for-sea-10793700>
- Kyodo. The Japan Times. "Singapore and Japan Ink Accord to Strengthen Cybersecurity Cooperation." 19 September 2017. Diakses pada 7 Desember 2018. <https://www.japantimes.co.jp/news/2017/09/19/national/singapore-japan-ink-accord-strengthen-cybersecurity-cooperation/#.XAqpOmgzBIU>
- Limelight Networks. "The State of Cybersecurity 2017 – Southeast Asia". 2018. Diakses pada 2 Agustus 2018. <https://www.limelight.com/resources/white-paper/state-of-cybersecurity-southeast-asia-2017/>
- Lee, Newton. "Counterterrorism and Cybersecurity. Total Information Awareness". Springer. New York. 2013. ISBN: 978-1-4614-7204-9 ISBN: 978-1-4614-7205-6
- Lung, Nicky. OpenGov Asia. "How Cyber Security Agency is Protecting Singapore In The Changing Cyber Landscape". 1 April 2018. Diakses pada 8 Desember 2018. <https://www.opengovasia.com/how-cyber-security-agency-is-protecting-singapore-in-the-changing-cyber-landscape/>

- McFadden, Christopher. "James Watt, Father of The Modern Steam Engine". Interesting Engineering, Culture/Biography. 30 Desember 2017. Diakses pada 18 Juli 2018. <https://interestingengineering.com/james-watt-father-of-the-modern-steam-engine>
- Mely, Caballero-Anthony, Alistair D. B. Cook. "Non-Traditional Security In Asia: Issues, Challanges and Framework for Action". Institute of Southeast Asian Studies. Singapore. 2013. ISBN : 978-981-4414-41-8. e-ISBN : 978-981-4414-60-9.
- Morgan, Jacob. "A Simple Explanation of 'The Internet of Things' ". Forbes. 13 Mei 2014. Diakses pada 18 Juli 2018. <https://www.forbes.com/sites/jacobmorgan/2014/05/13/simple-explanation-internet-things-that-anyone-can-understand/>
- Morsello, Barbara. European Association for The Study of Science and Technology. "Digitalization of Life – How Technology Redefine The Self in The Global Context". EASST Review. Volume 35(4). Desember 2016. Diakses pada 5 November 2018. <https://easst.net/article/digitalization-of-life-how-technology-redefine-the-self-in-the-global-context/>
- Murphy, Matt. The Economist. "War In The Fifth Domain". 1 Juli 2010. Diakses pada 22 November 2018. <https://www.economist.com/briefing/2010/07/01/war-in-the-fifth-domain>
- Parameswaran, Prashanth. The Diplomat. "ASEAN Cybersecurity In The Spotlight Under Singapore's Chairmanship". 2 Mei 2018. Diakses pada 11 November 2018. <https://thediplomat.com/2018/05/asean-cybersecurity-in-the-spotlight-under-singapores-chairmanship/>
- Rachman, Fadly Fauzi. Detik Finance. "Apa itu Teknologi 4.0?". 4 April 2018. Diakses pada 18 Juli 2018. <https://finance.detik.com/industri/d-3952668/apa-itu-revolusi-industri-40>
- Rouse, Margaret. TechTarget, Search Security. "Cybersecurity". Mei 2018. Diakses pada 6 November 2018. <https://searchsecurity.techtarget.com/definition/cybersecurity>
- Sanou, Brahima. , International Telecommunication Union. "Global Cybersecurity Index". 2017. Diakses pada 29 September 2018. [https://www.itu.int/dms\\_pub/itu-d/opb/str/D-STR-GCI.01-2017-PDF-E.pdf](https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2017-PDF-E.pdf)
- Subhan, Arief. The ASEAN Post. "Southeast Asia's Cybersecurity an Emerging Concern". 20 Mei 2018. Diakses pada 28 September 2018. <https://theaseanpost.com/article/southeast-asias-cybersecurity-emerging-concern>
- Sugiyono. "Statistika Untuk Penelitian". Penerbit: Alfabeta. Bandung. Maret 2016. ISBN: 978-979-8433-10-8
- Sund, Christine. "Towards an International Road-map of Cybersecurity". ICT Applications and Cybersecurity Division, Telecommunication Development Bureau, International Telecommunication Union, Geneva, Switzerland. Emerald Insight. 16 Juli 2007. Diakses pada 9 Desember 2018. DOI:10.1108/14684520710832306. <http://sci-hub.se/https://www.emeraldinsight.com/doi/full/10.1108/14684520710832306>

Tropina, Tatiana., Cormac Callanan. "Self and Co-regulation in Cybercrime, Cybersecurity and National Security". Springer International Publishing. Springer Briefs in Cybersecurity. New York. 2015. E-Book ISBN: 978-3-319-16447-2. DOI 10.1007/978-3-319-16447-2

University of Washington. Department of Global Health. Bryan J Weiner. About, Biography. 2018. Diakses pada 25 September 2018.  
<https://globalhealth.washington.edu/faculty/bryan-weiner>

Weiner, Bryan. BMC, Implementation Science. A Theory of Organizational Readiness for Change. 19 Oktober 2009. Diakses pada 26 September 2018.  
<https://implementationscience.biomedcentral.com/articles/10.1186/1748-5908-4-67?report=reader>

Weiner, Bryan. University of Washington. ResearchGate. "A Theory of Organizational Readiness for Change". Oktober 2009. Diakses pada 26 September 2018.  
[https://www.researchgate.net/publication/38021465\\_A\\_theory\\_of\\_organizational\\_readiness\\_to\\_change](https://www.researchgate.net/publication/38021465_A_theory_of_organizational_readiness_to_change)

Yu, Eilen. ZDNet. "ASEAN Countries to Established Framework for Cybersecurity Collaboration." 20 September 2018. Diakses pada 10 November 2018.  
<https://www.zdnet.com/article/asean-countries-to-establish-framework-for-cybersecurity-collaboration/>